Season1-Episode:
Remote work in 2023 with James Fair

Journey into the future

Always on Fridays, Xenia uses the “Let’s Work” Co-Working spaces in the city to work from there. She enjoys being surrounded by other professionals to have coffee breaks, or to at least not be disturbed at home by the kids and Thomas, her husband.
While she is standing at the coffee machine in the kitchen of the building, her friend Anna starts telling her how stressed she was the day before with online meetings all day and her family at home, being noisy in the background.
“Oh yes, Anna, let me tell you a story!”, Xenia immediately says. She starts sharing her experience from that one day in March back in 2020. The pandemic had just started, and it was her second week in her home office. While she was hiding from the rest of the family in the bedroom, she was scrolling through her Email Inbox. One Email caught her attention. The title stated: “Your office is contaminated by Coronavirus – Another of your colleagues infected”. Xenia immediately felt anxious and was worried about her and her family's health. She did not think twice. Xenia opened the Email and clicked on the attached link to get more information. But suddenly her computer turned black and a pirate skull popped up on the screen. In that moment she realized, she became a victim of one of these phishing scams, she heard so much about when the pandemic started.
After she had calmed down, Xenia called the security helpline from her company to report the case. Fortunately, her colleague on the helpline revealed to her, that the phishing email was only a test from her company to raise awareness among the staff. The laptop was functioning normally again, after one hour.
"And after all that, Anna, listen to what topped the day off. In the afternoon, I was on a videoconference and not muted. Started to discuss the numbers of the month with my team, suddenly Thomas opened the door to our bedroom and screamed in excitement for everyone to hear: “Darling, can you imagine? I finally got toilet paper in the supermarket!”.
After Anna and Xenia had a good laugh, back in the co-working office, Xenia opens her laptop and starts scrolling through her Emails, thinking to herself how grateful she is for having a secure internet connection and an optimal working environment here at “Let's Work”.

Agnes Kunkel: Hello, I'm Agnes Kunkel, your host in the 2023 podcast, your window to the World Beyond covid-19. Today we are just about hitting twenty four point two million confirmed cases worldwide and over eight hundred and twenty six thousand people have been confirmed to have died from covid-19. It's so sad to hear from episode to episode that these figures are still so dramatically rising. But the curve of new daily infections seems now to fall slightly, and we are still below 300 cases per day. What will happen during the next month, especially here in the Northern Hemisphere, where people tend to stay inside more? Today is the twenty seventh of August 2020.

Our guest today is James Fair, the senior vice president of technical operations at Secure Tech Executech, who is a leading I.T. service provider. Fast growing, as I understand, in your area, in the West and Midwest. And you have been for many, many years in the industry. And you have seen, I guess, a lot, but not anything like covid-19. James, welcome here to our podcast. We are happy to have you here with us to talk about remote work and the technical side of cyber security. In 2020, nearly half the world moved to the Home Office very unexpectedly. What did this mean for your company?

James Fair: Thank you. First of all, it's a pleasure to be here. Thank you for the invitation and thank you to your audience.

For us, it was, briefly at least, a huge boom. Most of our world certainly wanted to move to a work from home environment. So there was a massive scramble to buy laptops, to buy webcams, to buy headsets and to get VPN licenses so they could connect securely to their work environments. So we had a huge upturn in the amount of work. Everyone was scrambling and busy and everyone kind of looked like a deer in headlights for a little while. They were in like a panic mode. So, yeah, it was actually a big boom for us for quite a while.

Agnes Kunkel: You managed to have the people to manage the boom.

James Fair: We did. So Executech runs two different models with the traditional remote support model and we also have an onsite group. So we were able to make the shift fairly well. We had a model of remote people that kind of showed us what to do and how to do it well.

Was it stressful? Yeah, absolutely. Most of the staff was having to leave their home. We had people working from home and suddenly they had children at home. And that's both a blessing and a curse for a lot of people I'm sure.

Agnes Kunkel: I guess it was really hard to handle this, a boom and staying at home at the same time?

James Fair: I think so, yeah. There was a lot of stress I know. Now I'm older and my kids are adults, but we have a puppy that was supposed to have been my wife's dog, but she and I totally bonded. So I've got this tiny dog with me all the time now. A few months before the pandemic hit, I'd been kind of feeling guilty about leaving the house, because she gets this *really* sad look on her face, and it makes me feel guilty. And when I come home to her, she is super excited to see me and she would run around. No one else in my household treats me that way when I get home. I was leaving one day and I thought, “I wish I could just work from home.” And I suddenly got my wish, in a really big way. Then I discovered that there are some challenges with working from home, she always wants to play (she bothers me all the time), when my wife wants to have a conversation, when I'm in the middle of a webinar, for instance. My wife's very understanding about workload, but still, it's tough to kind of juggle all this. And that's just without children. My son and daughter-in-law and their two kids live below us, and I've seen them struggle a lot. It was tough for them to have children at home, to be working at home and trying to juggle all those things at the same time.

So, I think we've seen people adjust now. A lot of people I think are feeling better and are getting more used to this new routine. Humans are very resilient. And it didn't take long before the staff really adjusted to both home life and work as well.

Agnes Kunkel: It's just as you say, I heard in another interview that people are very resilient, they can adapt very quickly. And when it's the motto, you have to go and stay at home and manage in some way, we do. And when we have to go to the office again. We will manage too.

From your expertise now and from the I.T. support side, have you been happy that your clients moved to remote work in a big number? Isn't it risky to be in the living room, kitchen or whatever, and connect to unsecure WiFi. This must have been challenging.

James Fair: Yeah, definitely. Some security challenges came with that. Most people at home aren't going to spend a lot of money on a new, modern firewall. What we call a deep packet inspection firewall that's going to look at all the packets going in and out. They're usually using whatever their Internet provider is providing, and their home computers typically aren't set up nearly as securely. They may not want to spend the money for an expensive antivirus program like your corporations or organizations would. And, although it's not very common in homes, theft could be an issue. So, if I'm saving client data to my home computer and my home computer gets stolen, that data is now accessible, whereas most corporations and organizations will encrypt the hard drive - that kind of thing. And as you've mentioned, wireless is a big challenge. Wireless is not secure. It's not set up by technical people at your home.

Agnes Kunkel: So let's come back to the nightmare. You said that this was in some way a nightmare for people working in the security of IT.

James Fair: Yeah, so if your job is to make sure that the staff of your organization is always secure or as secure as possible, how do you do that when they're not at the office? How do you do that when they're at home on a computer that's potentially used by other people? I may trust the employee to be safe, but how do I know that person's spouse or their children, who also use the computer, are going to practice those same safe habits. So, it has become a big challenge for security people to try to ensure some or an approximate level of security that existed before we all went home.

Agnes Kunkel: Are there new tools, new ideas used to achieve this level of security you need for your company?

James Fair: We haven't seen anything necessarily new that addresses this just yet, I'm sure there will be. That's going to be a huge market. I don't doubt that many of those products will start coming out. I'm sure it's going to be a huge market. For now, it's a bit of a scramble to try to get us somewhere near there. And then there's the challenge of

“is it OK for me to put my tools on your home computer?”. Are there legal ramifications to doing that? It's a lot to consider. So, it can be very challenging.

Agnes Kunkel: I understand. And wasn't there a tradeoff between letting people go on with work in a not so secure way?

James Fair: Unfortunately, security and ease of use are really at opposite ends of the spectrum. The most secure computer in the world is the one sitting in the middle of the room unplugged with no wires attached, but it's very unusable. So, we try to find a balance between what's easy for people to use and what's more secure. And we see that security's all about layers. The more layers I can put in place, the more effort it will require the attacker to get through in order to be effective. For instance, multifactor authentication, hopefully everyone is using that. If you're not, I would certainly recommend everyone use it. It's a fairly quick and easy layer of security that provides not just username and password anymore, but one more layer. I'm going to pick up my phone or look at an app or do something else. So, it's an additional layer.

How do we balance more security and still make it easier for the user without being cumbersome? Because, if you make it too cumbersome, they will simply bypass it. They'll stop using it. They'll find a way around it. They'll circumvent your security. So, it is very much a juggling act. And we had to get people to work. So, in a lot of cases, it was like, look, just go home, go to work and we’ll try to figure this out as we go.

Agnes Kunkel: Oh, so did it work well, that your clients didn't get harmed in some way or did you see some problematic issues where companies had problems arising from that?

James Fair: I would say generally we've been very successful. There was an awareness change as well: people realize this is an issue. So, I think for some the awareness increased and people were more sensitive around that. We didn't have a whole lot of incidents other than someone goes home and now they have technical challenges. Well, they may not be anywhere near the office, so I can't really help you plug in your printer remotely. Some of these are physical challenges.

Wireless isn't as fast as wired. So connection may be slower. But overall, I would say that there was a scramble from all MSPs, not just us. To get people working from home was pretty successful. Most of the world is working from home now. So, I'd say we did pretty well, all in all.

Agnes Kunkel: Yes, global I.T. support and especially your company did really well to make this work.

You just talked about rising awareness of the employees on the risks in our little story at the beginning there is like a fire drill. Where a company simulates attack. Is this common?

James Fair: Yeah. So, I appreciate you asking this question. Actually this subject is pretty near and dear to me. I do a lot of public speaking on what it takes to secure an organization. And, as I mentioned before, most companies have put a lot of security features in place. So unfortunately what has shifted is the attackers have realized that it's tough to get through a firewall, antivirus and all these other things we've put in place. But the busy people who are now working from home, possibly juggling children at home, unused to this working from home environment, they're on their 200th Email message for the day and they're not being super careful. So, these hackers and attackers - these criminals- they're finding the easiest target which is, unfortunately, the very busy people who can make mistakes. A firewall may not ever make an error, but humans do. There's always human error. So, for us in security, we want to remind people that this is a common attack method.

These days, these hackers are trying everything they can to get you to click on the wrong thing and open the wrong program. Like I said, security is about layers. And very early in my career, I learned this the hard way. I had this belief that if I secured the outside world against the inside world and just protected these kinds of gateway points, that we would be secure. And I unfortunately learned a very big lesson that that was not true, because all it took was one time to get through and everything inside was suddenly infected. And we had to touch a thousand computers by hand. So much earlier in my life I learned that that's not OK. We've got to protect the inside as well. We want to create as many layers as possible. That makes sense in terms of ease of use cost.

But back to the original question. Yeah, it's pretty common these days now for us to simulate that attack in order to raise awareness. I can't tell you how many clients we have do this to. And suddenly, for the next several months, every email that's suspicious is sent to the IT group asking “Is this OK? Is this legitimate?”. I'd rather have them ask me a hundred times than click on one they shouldn't.

Agnes Kunkel: So you recommend raising awareness of your employees on these issues through fire drills and these tests, so everyone understands how important it is. You talked about secure WIFI let's talk about this in comparison to not secure WIFI in a remote work environment?

James Fair: So, we've seen wireless and security progress. Each progression, unfortunately, was kind of due to the previous one getting cracked or hacked or attacked, and it's kind of this cat and mouse game where someone creates a new secure method of doing wireless. And then and we all adopt that. We make all our equipment change and we all hopefully do security updates. But then eventually someone comes out with another way to break that one. And part of this is due to that Moore's Law where the computing power is going up exponentially. So perhaps what would have taken months to crack a cryptographic algorithm, now only takes hours. And this industry so far has been very reactive. I've been around a long time, three decades, and I don't believe I've ever seen a progression in wireless that wasn't because of someone breaking the previous one. So, we scramble to replace gear, upgrade existing gear, put on new firmware and adopt these new things. And unfortunately, what we see often is there's some old device that must be part of the company culture, or company organization that still has to be supported. So, then they keep that insecure method and eventually that can be cracked or broken or attacked. So, I know it's a pain, but I really have to suggest wired as the answer. You can't break into my wire unless you're physically in my home. But if I'm outside of your home, I can probably get into your wireless. No I know you can't get up and move around and go outside without it, but wireless is subject to noise. Only so many devices can attach. At the same time, we have bandwidth challenges. So again, I say it's a pain, but I always recommend going wired whenever possible. With wireless, it’s just a matter of time before the version we're using now will be cracked again.

Agnes Kunkel: It's not nice to hear, but maybe it's good to hear this. So you say wireless might be OK for Netflix, but not for work.

James Fair: Correct.

Agnes Kunkel:(laughs) Then I have to think about my own usage.
Cloud is another fancy aspect. When everything is in the cloud, it's wonderful. We have people in remote places with whom we can collaborate in the cloud. What does IT security speak of the cloud?

James Fair: I've actually had this conversation with many. It's an excellent question, so first of all, thank you for that question. I've had that question brought up by many organizations - typically ones run by some older generations - who are unfamiliar with the cloud. They don't trust it. They feel like it may be less secure. And I don't want to set any false expectations. Every platform, no matter what we're using, is going to be subject to exploitations and hacks. But think about it this way. So, first of all, the physical security: I've been in environments where the server was in the same closet with a water heater or companies that went under because there was a break-in and all equipment was stolen and they had nothing to go on. So now in our traditional server environments, we're hopeful that our firewall is doing its job and that your I.T. administrator is doing the windows updates and filling these holes that are being discovered. But how frequently is that happening? Is it frequently enough? And then is someone monitoring for malicious activities? What about backups? When was the last time someone reviewed the backups? It's far too often that we go to an environment and we see that the old server was being backed up, but not the new one. And the new one was the one that has the struggle.

Now let's consider companies like Microsoft and Google and Amazon that are hosting these massive cloud environments, that are in crazy secure facilities. I have been to a data center and it takes a lot to get into one of these. And they have redundant everything: redundant power, Internet, and the ability to shift resources. So, if my server dies, I never even know it. It just shifted to another hardware platform. And I never even know. I don't miss a beat the whole time. They've got a massive security team that are monitoring because it's their reputation on the line. If they get hacked, they're going to throw a lot of resources at making sure things stay secure. And if an event does

happen, they have massive resources they can throw at it to try to get it fixed. The truth is, nothing is secure forever and you have to keep fixing these holes and patching things. And these companies are really, really good at that. And they do it timely. They're watching for these things because their reputations are on the line. Cloud can be, in some ways, even more secure than our on-premise server rooms.

Agnes Kunkel: Ok, so you say professional data centers are good, as they are professionally managed, and have much more resources on the issues we are talking about, than you typically have maybe in a mid-sized company.
When we think about bringing the data from the datacenter to the remote places. Is there anything we have to watch out for or how to transfer the information in a secure way to the remote workplace?

James Fair: That is definitely an environment we see that progresses all the time. We are constantly trying to improve the connection and make it more secure. The world has been pretty good about phasing out protocols that aren't supported or are insecure. But I would say VPN is singularly the most secure method of transmission. We can create a connection between our laptop, desktop - whatever we're using - and the facility we're connecting to over the Internet. But because it's encrypted it's our own private connection, it's not subject to being viewed. No one can pull those packets out and see what's inside of them. So far, that's been a very secure and highly recommended method of transmitting any kind of data that should be secure. And it works very well.

Agnes Kunkel: Should everyone who is a working remote be connected via VPN?

James Fair: There's a couple of different scenarios here, so I would say if you are directly copying data or moving data from your computer at home to someone's organization, absolutely. There are also other alternatives where you can connect remotely to a computer and you're not actually network attached. Instead, you're just doing screen connections and mouse clicks. So, that remote computer can't ever get any kind of data. It won't transmit data to you. You're not transmitting data to it. All you're doing is screen information. So that's also very secure and works very well.

Agnes Kunkel: But as long as you have a mirror to your SharePoint on your local machine, then it would be preferable to have a VPN.

James Fair: Always.

Agnes Kunkel: I learned so much. We have to turn IT Security upside down after this interview. You hear about it and you think it's just maybe for big companies. But in the end, everyone has to watch out for these things.

James Fair: Yeah, these small organizations are targets because they typically have less resources and fewer security methods in place. So, unfortunately they're often the targets these days.

Agnes Kunkel: Another aspect of securing local machines is about face recognition or voice recognition. What do you think about these ideas or possibilities?

James Fair: I think they're great! As I talked about before, this idea of ease of use and security being at opposite ends. I would layer on eight layers you have to go through before you get in, just to make sure it was really you. But it'd be so hard for you to work. You would throw things at me and you would not like me very much. So instead, I can use your face or nowadays Windows is using Bluetooth connections.

So, as I approach my computer, it'll make a Bluetooth connection and will unlock, because it knows it's me. And if I step away, it locks it. I love the idea of anything that makes it easier for the end user to log in but still be secure: anything like face ID, voice recognition. Although it's not full proof. If I was under duress, if there was someone holding a gun to me physically, it wouldn't secure me. But it is far better and far easier. Which, again, we want it to be easier for the end users, so they're going to use it and adopt it. That's definitely a plus. I would say yes, one hundred percent.

Agnes Kunkel: So it should monitor your heartbeat rate, to check if you are in a good condition.

James Fair: If a gun is pointed at my head, that would be something.

Agnes Kunkel: Ok, I have read somewhere, that a face or a thump is just data in the end. What about if someone steals data from facial recognition or a thumb recognition?

James Fair: It's the same as any other secure data. Logins and usernames are available. Like if someone has a breach to those logins and passwords, they go on the dark web and sell them to other criminals. So that kind of information is always out there. Again, the answer is just layer them. It could also be that kind of data will also be stolen and sold somewhere. But if we have multiple layers, then hopefully it's very difficult to coordinate all those and make them work together.

Agnes Kunkel: Yeah, but there is one slight difference. Maybe if a fingerprint is stolen. I can take another one, but I cannot switch my face when it's stolen (laughs).

James Fair: (laughs)That is very true. You can't recreate your face. We don't want you to, you have beautiful face, we don't want you to change that.

So, there will probably be a point when we see that facial recognition methods will also change. Not the data itself, but the method of transmission that we're using. So, a lot of times the protocols - the methods that we use to transmit - they will have to change. And that's very common. The methods which transmit passwords nowadays are very different from what you used to use 20 years ago. Passwords can still be stolen, but now the transmission method is much harder to break and get into. There's a downside to every method we use. The idea is to try to stay ahead of these criminals. That's the best we can do.

Agnes Kunkel: Yeah, but especially this idea of when one's face is compromised in that way, it's really difficult to replace. Maybe you should use just part of the face that might be a chart or the pattern of skin. Then you can say, OK, well, this is compromised. We can just use the tip of the nose.

James Fair: Or maybe the technology will improve. And pretty soon we can read our retinas, which is even more detailed than our thumbprints. Technology tends to change when there's been a breach or crack in some kind, like in wireless. So then someone smart comes out and says, I've got a better way to do this. Hopefully we keep doing that.

Agnes Kunkel: Yeah. I's still a “catch me game - runaway and catch me”. And it's done for all times. When you think about these remote workspaces that you mentioned already, what do you think of the hardware problems.

James Fair: Yeah. It's a real challenge. We have a lot of remote support people who can handle the majority of your tasks. But if a device gets unplugged, that's a real challenge. How do I get there? There are a couple of different options. I worked with a company who deployed an onsite field technician. This company's job is just to collect all these field technicians and review them and rate them. And then you could go and say “I want that person to go to your house and help you out”. Now however, there is this pandemic's challenge. Maybe you don't want that person in your house now. But assuming you're open to the idea of having someone in your house. I can contract that work out. And I want to make sure it's someone we've vetted, someone we know is not a criminal themselves. We do some vetting and these companies are very good about that. They do vetting and reviewing. And you can see all the past reviews of a technician, all the work they've done, and then choose the person you want to go out there. That's one possible option. The other one is, if you're willing, in a lot of cases I can ask you to be my remote hands. Will you please use FaceTime or Teams so you can show me what it looks like? And I'm going to try to get you to walk through the process to plug-in this cable. It's painful, but we've got to be able to adapt to this environment that we're in now.

Agnes Kunkel: There are solutions to this problem. When we think about 2023, quite a lot of our guests talked about workspace sharing, you are not working in your own home. You go to a coworking space.

Agnes Kunkel: When I thought about our topic, I thought this might be a place where you could be a little bit more secure from the IT side. And maybe these centers could be able to have someone who was doing the physical side, maybe looking for Router, looking for Printer or local machine for whatever might happen. Do you think that coworking spaces are a part of the solutions for the new working world in 2023?

James Fair: Yeah, I do. We've seen a lot of success here in the United States with them, they really took off. There's a lot of empty office space, particularly now, that could be leveraged by people to go somewhere to have, as you said, a secure

infrastructure already created. You still want to make sure, because there's a bunch of people there, that your connections are safe. Your virtual private connection, your VPN and other tools. But, yeah, you've got the infrastructure in place. And these companies go through a great deal of effort to make sure that it's easy to connect to the conference room, computer or the printer. They want to make sure it's easy, otherwise you go somewhere else. So they're really focused on supporting those people in those environments. I think it'll be a great solution moving forward.

Agnes Kunkel: As it looks to me like a nice mixture of a professional environment and avoiding commuting. It's going to very expensive downtown office towers. And yes, I wouldn't be surprised if we really see much more of this in the next years like 2023.

James Fair: And sure, it`s cost too. I don't have to pay for a full office building. I can have a small one. And if I grow or expand, I can get a couple next door. And we can kind of flex with what we do with the cloud resources. So, yeah, I definitely see us leveraging this more in the future.

Agnes Kunkel: Do you have an idea what players might move into this business opportunity?

James Fair: I think we're seeing more of that because I think a lot of organizations are deciding that, hey, this work from home stuff… this works. People seem to be happier (once they adjusted). As you mentioned, the commute time drops to zero. So, all those big empty buildings are going to be available. And I could see a lot of places going "yeah, let's turn this into a shared space, because we're not selling it as a one big unit". So instead, turning it into a shared environment and share some of the costs among lots of people. Here in the States, we had a few different players already in the space. There's a building not far from me - great, huge thing - and in was going a second one. It was a pre-pandemic, but this was WeWork. I think they've had some financial difficulties. Don't quote me on that. But we definitely see some big players coming into this space going, "yeah, this is this is the future."

Agnes Kunkel: I wouldn't be surprised if some big players, say maybe from the facility management side, as they are ready to do this, the hardware side from this business, that they would be the one who could move into this space.

Yes. When we now summarize for our listeners, what would be your summary? What should we expect in the next two to three years on the aspect of I.T. security, remote work, shared working spaces, clouds? What should we be prepared for?

James Fair: Well, we're definitely seeing a trend toward, as you mentioned, the cloud, that's a big one. We're also seeing a trend where people are not going back to work. Major organizations like Google and Microsoft have said, “yeah, just stay home”. I believe I saw a memo from the president of Google, the CEO, and he said “probably October we may reassess. But for now, we may allow like one sixth of the staff back and in kind of a rotating fashion”. But this working from home thing is great. And I think of parking and commuting and frankly, the pollution that's created by all that commuting. And this is definitely a trend I think we're going to keep going. We've discovered that it works. It was tough and we had to adjust, but as you mentioned, humans are resilient and we're going to adapt and we're going to realize that, “man, this is kind of nice. I can stop talking to you, walk into my kitchen and have lunch and I don't have to go drive somewhere to get food”.

So, cloud computing is a big one. We going to see some companies that start to come up with some methods or some solutions for securing your home environment. How do I create maybe a subset of my work computer or my home computer, rather, that's just for work and it's secure from everybody else who uses my computer? I definitely think we're going to see solutions around that very soon.

We've seen bandwidth increases as people worked from home. All of a sudden, all the Internet providers around the world strained under that additional load. Higher bandwidth, I think deployments of 5G. Deploying 5G's one of big things. That could be a game changer for a lot of people, although it will take a long time. But could potentially be a big game changer. I would love to go work at the park instead of sitting in my office all the time.

Agnes Kunkel: Who wouldn't like to go to the park instead of sitting inside! When you look back to the time of the pandemic, the changes you have made to your personal life, what are the things you would like to keep even after the pandemic, to increase your life quality, life-work balance?

James Fair: I like working from home, it took some adopting. I have to share the dog duties with my wife now. Children at home has also been a struggle for a lot of people. But it can be really a game changer, particularly if they're at home. Who's going to watch the children if we're not at home. We had some people who had to say, “I have to go work from home. I have no choice in the matter. My children are home” at least here in the States.

On the downside, I would say unfortunately, probably we will see more of these kinds of criminals. They're going to keep leveraging this. When the world is in chaos, bad people don't have the moral feelings that hopefully most people do. And it bothers me that they do this. But they see this as an opportunity. And it makes me want to fight those people even more.

At a personal level, I run a big team. I've seen a big insight on how challenging it is for those that rely on finding external certainty in their life. I kind of saw the split - this divide when this thing hit - where people that are more secure inside themselves did pretty well. And there were people who kind of relied on the outside world and its consistency. They did not do so well. And there was a lot of anxiousness around that. So hopefully we're going to see some more adjustment for people like that who are struggling at this time. Like I said, I got to see firsthand the stresses that it puts on a family with parents working from home and children at home. So, for me personally, I learned a lot of tolerance and a great deal of patience. I had to learn that not everyone will handle this the same. Not everyone will adapt to it as quickly. And I hope that others find some room for tolerance and understanding, because everyone does deal with this differently.

Agnes Kunkel: Sounds like a wonderful leadership lesson.

James Fair: I think so. Thank you.

Agnes Kunkel: Ok, but was a wonderful summary from your side and thanks a lot.

I have learned lots and tons of stuff about IT. And I think I will accept your advice on change bit here in our company. And of course, we wish you and your team and your

company good times ahead and many successes and nice growth. And thank you, James for being with us.

James Fair: It's my sincere honor to serve and I hope your audience gets value from it and I hope you do make those changes in security. Thanks very much for having me on the show. Have a great day!

Agnes Kunkel: Thank you. Bye bye.